Myth: OSS community does not lose to crackers

Yuto Uenaka (Kyushu University)
Masanari Kondo (Kyushu University), Shinobu Saito, Yukako Iimura (NTT), Naoyasu Ubayashi, Yasutaka Kamei (Kyushu University)

Background: Linus's law [1]

Linus's law

Given enough eyeballs, all bugs are shallow

Myth

OSS community take less time to resolve vulnerabilities

[1] Eric Raymond. The cathedral and the bazaar. Knowledge, Technology & Policy, 12(3):23–49, 1999.

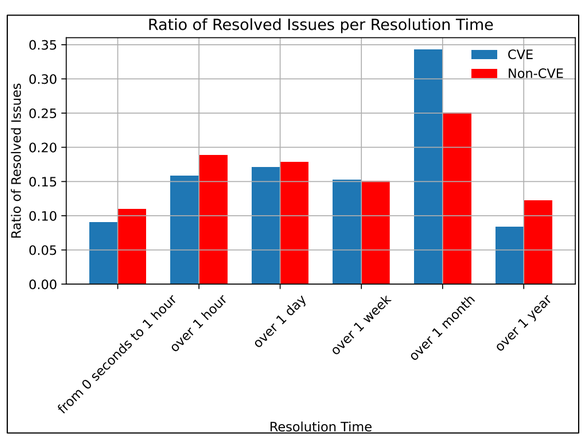
Target data

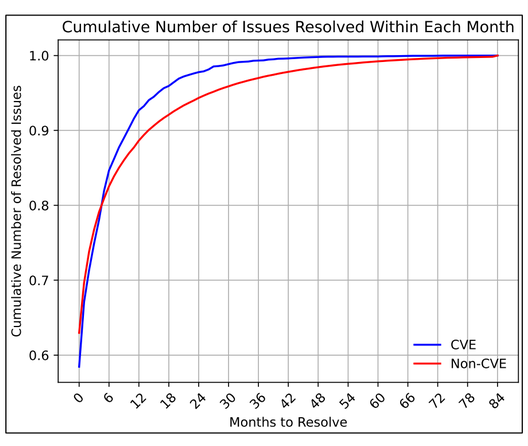
Features	Value
#Repositories	225
#Issues	1,227,442
#Issues related to vulnerabilities	7,465
#Issues non-related to vulnerabilities	1,219,977
#PRs	1,525,604
#PRs related to vulnerabilities	6,875
#PRs non-related to vulnerabilities	1,518,729

Analysis 1

We investigated the resolution time for both vulnerability-related and non-vulnerability-related issues

Resolution time = Resolution date – Creation date





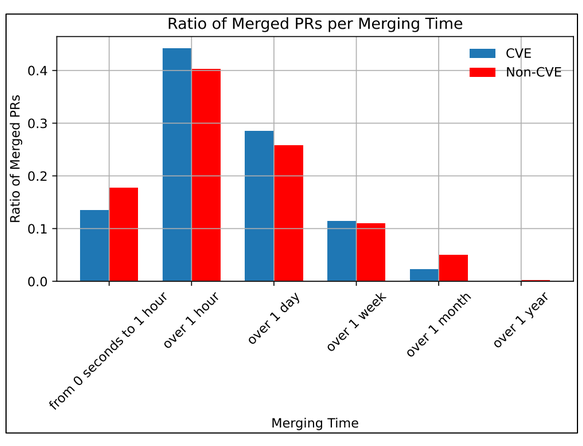
Finding 1-1: The left figure indicates that the proportion of issues resolved within one year is higher for vulnerability-related issues. The right figure further shows that the resolution time is relatively shorter for these issues.

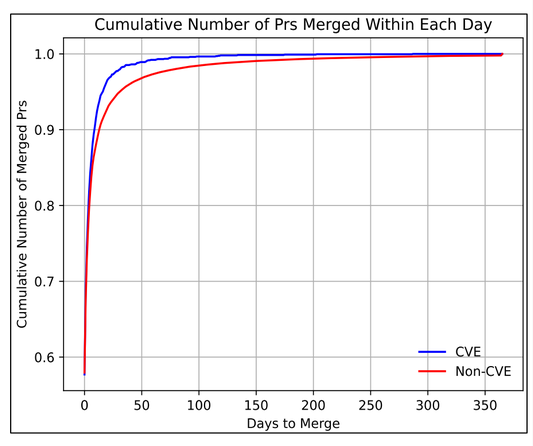
Finding 1-2: The left figure shows that the proportion of resolved issues within one day is higher for issues unrelated to vulnerabilities.

Analysis 2

We investigated the merge time for both vulnerability-related and non-vulnerability-related PRs

Merge time = Merge date – Creation date





Finding 2-1: The left figure shows that the proportion of merged PRs within one month is higher for vulnerability-related PRs. The right figure further shows that the merge time is relatively shorter for these PRs.

Finding 2-2: The left figure shows that the proportion of merged PRs within one week is higher for PRs unrelated to vulnerabilities

Fact, Discussion

Vulnerabilities are resolved quickly in OSS community

Possible reason for Finding 1-1, Finding 2-1

- OSS developers have a high level of awareness regarding vulnerabilities

Possible reason for Finding 1-2, Finding 2-2

- Difficulties of issues
  - The difficulty of vulnerability-related issues may be higher than that of other issues.
  - In contrast, issues unrelated to vulnerabilities may include relatively easy ones

Additional analysis

The relationship between vulnerabilities severity and issue resolution time

We assumed that if developers have a high level of awareness regarding vulnerabilities, they would be more likely to resolve those vulnerabilities. However, no significant correlation was found.

The relationship between issue resolution time and the number of comments

We assumed that if developers have a high level of awareness regarding vulnerabilities, they would be more likely to discuss vulnerabilities in issue threads. However, we found that discussions are more active in issues unrelated to vulnerabilities.

Issue and PR inclusion

Vulnerabilities need to be handled with caution, and the process of first creating an issue before opening a PR is generally followed to ensure proper management. However, this structured process is only observed in 13% of cases involving vulnerabilities.